



guía de gestión de equipos de sobremesa

estación de trabajo hp xw4000

estación de trabajo hp xw6000

Número de referencia del documento: 301201-071

Octubre de 2002

En esta guía encontrará definiciones e instrucciones sobre el uso de las funciones de Intelligent Manageability y seguridad preinstaladas en determinados modelos.

© 2002 Hewlett-Packard Company

Compaq, el logotipo de Compaq, ROMPaq y iPAQ son marcas comerciales de Compaq Information Technologies Group, L.P. en los Estados Unidos y en otros países.

Microsoft, MS-DOS, Windows y Windows NT son marcas comerciales de Microsoft Corporation en los Estados Unidos y en otros países.

Intel, Pentium, Intel Inside y Celeron son marcas comerciales de Intel Corporation en los Estados Unidos y en otros países.

Todos los nombres de otros productos mencionados en este documento son marcas comerciales de sus respectivas empresas.

Hewlett-Packard Company no será responsable de los errores técnicos o editoriales contenidos en este documento o de los daños resultantes o secundarios relacionados con la provisión, rendimiento o uso de este material. La información en este documento se proporciona "tal cual" sin garantía de ningún tipo, incluidas, pero sin limitarse a, las garantías implícitas de comercialización y mantenimiento para objetivos concretos, y se puede cambiar sin previo aviso. Las garantías para los productos HP están estipuladas en las declaraciones expresas de garantía limitada que acompañan a dichos productos. La información contenida en este documento no debe interpretarse como una garantía adicional.

Este documento contiene información de marca que está protegida por copyright. No se puede fotocopiar, reproducir o traducir a otra lengua ninguna parte de este documento sin el consentimiento por escrito de Hewlett-Packard Company.



ADVERTENCIA: Cuando el texto aparece de este modo, significa que si no se siguen las instrucciones pueden producirse lesiones e incluso la muerte.



PRECAUCIÓN: Cuando el texto aparece de este modo, significa que si no se siguen las indicaciones se puede dañar el equipo o perder información.

guía de gestión de equipos
de sobremesa

estación de trabajo hp xw4000

estación de trabajo hp xw6000

Primera edición (Octubre de 2002)

Número de referencia del documento: 301201-071

Contenido

Guía de gestión de equipos de sobremesa

Configuración y distribución inicial	2
Remote System Installation	3
Actualización y gestión del software	3
Altiris eXpress	4
Altiris eXpress PC Transplant Pro	6
Altiris eXpress HP/Compaq Client Manager	6
System Software Manager	7
Product Change Notification	7
ActiveUpdate	8
Memoria flash de la ROM	8
Memoria flash de la ROM remota	9
FailSafe Boot Block ROM	9
Replicación de la configuración	12
Botón de alimentación de modo dual	13
Power Management	14
Página Web	15
Productos base y empresas colaboradoras	15
Desktop Management Interface (DMI)	16
Wired for Management	16
Seguimiento y seguridad de activos	17
Seguridad mediante contraseña	20
Eliminación de una contraseña de arranque o de configuración	25
Modo de servidor de red	26
DriveLock (Bloqueo de la unidad)	27
Sensor de Smart Cover	30
Bloqueo de Smart Cover	31
Master Boot Record Security (Seguridad del registro de arranque maestro)	34
Candado con cadena	37
Tecnología de identificación de huellas digitales	37

Notificación y recuperación de fallos	38
Sistema de protección de unidades	38
Seguimiento de la integridad de discos Ultra ATA	39
Fuente de alimentación con protector de sobretensión	39
Sensor térmico	39

Índice

Guía de gestión de equipos de sobremesa

La empresa HP fue pionera en la manejabilidad de equipos de sobremesa con la introducción en 1995 de los primeros equipos personales de sobremesa completamente manejables de la industria. Desde entonces, HP ha realizado grandes esfuerzos para desarrollar los estándares y la infraestructura necesarios para distribuir, configurar y gestionar de forma efectiva equipos de sobremesa, estaciones de trabajo y ordenadores portátiles. Intelligent Manageability de HP proporciona soluciones basadas en estándares para gestionar y controlar equipos de sobremesa, estaciones de trabajo y ordenadores portátiles en un entorno de red. HP trabaja en estrecha colaboración con los proveedores de soluciones de software de gestión líderes en la industria para garantizar la compatibilidad entre Intelligent Manageability y estos productos. Intelligent Manageability es un aspecto importante de nuestro compromiso general de proporcionarle soluciones para el PC que le ayuden durante las cuatro fases de éste: planificación, distribución, gestión y transición.

En esta guía se resumen las capacidades y funciones de los siete componentes principales de gestión de equipos de sobremesa:

- Configuración y distribución inicial
- Remote System Installation
- Actualización y gestión del software
- Memoria flash de la ROM
- Productos base y empresas colaboradoras
- Seguimiento y seguridad del activo
- Notificación y recuperación de fallos



Las funciones específicas admitidas que se describen en esta guía varían según el modelo o la versión de software.

Configuración y distribución inicial

Los equipos se entregan con una imagen de software del sistema preinstalada. Después de un proceso muy breve de “desempaquetado” del software, el equipo está listo para ser utilizado.

Si lo desea, puede sustituir la imagen de software preinstalada por un conjunto personalizado de software del sistema y aplicaciones. Una imagen de software personalizada puede distribuirse de varias formas. Por ejemplo:

- Instalar aplicaciones de software adicionales tras desempaquetar la imagen de software preinstalada.
- Mediante herramientas de distribución de software, tales como Altiris eXpress, Microsoft MS Batch o Microsoft NT Distribution Share (NTDS), para sustituir el software preinstalado por una imagen de software personalizada.
- Mediante un proceso de clonación del disco para copiar el contenido de una unidad de disco duro en otra.

El mejor método de distribución depende del entorno y los procesos de tecnología de la información. En el apartado PC Deployment (Distribución del PC) de la página Web Solutions and Services (Soluciones y servicios) (<http://www.compaq.com/solutions/pcsolutions>) se proporciona información sobre cómo seleccionar el mejor método de distribución. También encontrará guías y utilidades para integrar herramientas de distribución basadas en Microsoft o PXE.

El CD *Compaq Restore* (*Restauración de Compaq*) o *Restore Plus!* (*Restauración Plus!*), la configuración basada en la memoria ROM y el hardware listo para ACPI proporcionan más ayuda en la recuperación del software del sistema, la gestión y solución de problemas de configuración y la gestión de la alimentación.

Remote System Installation

La función Remote System Installation sirve para configurar el sistema mediante la información de software y configuración localizada en un servidor de red. Esta función se utiliza generalmente como una herramienta de configuración del sistema y puede utilizarse en las tareas siguientes:

- Distribuir una imagen de software en uno o más PC.
- Dar formato a la unidad de disco duro.
- Instalar software o controladores de aplicaciones.
- Actualizar el sistema operativo, el software de aplicación o los controladores.

Para iniciar Remote System Installation (instalación remota del sistema), pulse **F12** cuando aparezca el mensaje F12 = Network Service Boot (F12 = Arranque de servicio de red) en la esquina inferior derecha de la pantalla del logotipo de HP. Siga las instrucciones que aparecen en la pantalla para continuar el proceso.

HP y Altiris, Inc. se han asociado para proporcionar herramientas diseñadas para facilitar la tarea de distribución y gestión del PC corporativo y reducir el tiempo invertido en ella, y básicamente para reducir el coste total de propiedad y hacer de los PC de HP los PC de cliente más manejables en el entorno de empresa.

Actualización y gestión del software

HP proporciona varias herramientas para gestionar y actualizar software en los equipos de sobremesa y las estaciones de trabajo, como por ejemplo, Altiris eXpress, Altiris eXpress PC Transplant Pro, Altiris HP/Compaq Client Manager, System Software Manager, Product Change Notification y Active Update.

Altiris eXpress

HP y Altiris han ampliado su acuerdo de colaboración para proporcionar soluciones líderes en la industria que reduzcan la complejidad de gestionar hardware y software para equipos de sobremesa, ordenadores portátiles, dispositivos de bolsillo y servidores a lo largo de su ciclo de vida. Altiris eXpress permite al administrador del sistema crear y distribuir rápidamente una imagen personalizada de software estándar de la empresa en uno o más PC de cliente conectados en red mediante una interfaz tan simple de utilizar como Windows Explorer. Altiris eXpress admite Preboot Execution Environment (PXE) y Wired for Management de Intel. Mediante las funciones Altiris eXpress y Remote System Installation del equipo HP, no es necesario que el administrador del sistema vaya a cada nuevo PC por separado para distribuir la imagen de software.

Las soluciones Altiris eXpress son una manera eficaz y efectiva de automatizar los procesos existentes y abordar áreas problemáticas en el entorno de TI. Con la infraestructura basada en la Web de Altiris eXpress, dispone de la flexibilidad para gestionar los sistemas desde cualquier sitio y en cualquier momento (incluso desde un iPAQ Pocket PC).

Las soluciones Altiris eXpress son modulares y extensibles para abarcar las necesidades de los grupos de trabajo de la empresa. Se integran con otras herramientas de gestión de clientes de la industria y proporcionan extensiones a Microsoft BackOffice/SMS.

Las soluciones Altiris eXpress expandidas se centran en cuatro áreas de TI principales:

- Distribución y migración
- Software y gestión de operaciones
- Inventario y gestión de activos
- Help Desk y solución de problemas

En unos minutos, Altiris eXpress puede instalar una imagen de disco que contiene el sistema operativo, el software de aplicación y el cliente de Altiris eXpress sin necesidad de utilizar un disquete de arranque distinto. Con Altiris eXpress, el administrador de red puede:

- Crear una imagen nueva o modificar una anterior, o bien clonar un PC en la red que puede tener la imagen ideal.
- Crear cualquier número de imágenes de disco personalizadas para varios grupos de trabajo.
- Editar archivos de imagen y modificarlos sin tener que empezar desde el principio. Esto es posible porque Altiris eXpress almacena archivos en su formato nativo: NTFS, FAT16 o FAT32.
- Establecer un “evento de nuevo PC”, un script que se ejecutará automáticamente cuando se añada un nuevo PC a la red. El script puede, por ejemplo, dar formato a la unidad de disco duro del PC, crear una memoria flash de la ROM BIOS e instalar una imagen de software estándar completa.
- Programar un evento para que se ejecute en un grupo de equipos.

Altiris eXpress también incluye capacidades de distribución de software de uso fácil. Puede utilizar Altiris eXpress para actualizar sistemas operativos y software de aplicación desde una consola central. Cuando se utiliza junto con System Software Manager, Altiris eXpress también puede actualizar la ROM BIOS y software de controlador de dispositivo.

Para obtener más información, visite
<http://www.compaq.com/easydeploy>.

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro permite efectuar una migración de PC de forma sencilla ya que mantiene los valores, las preferencias y los datos anteriores, y los migra al nuevo entorno rápida y fácilmente. Las actualizaciones tardan solamente minutos en lugar de horas o días, y el funcionamiento y el aspecto del escritorio y las aplicaciones son los previstos por los usuarios.

Para obtener más información y detalles sobre cómo descargar una evaluación de 30 días totalmente funcional, visite <http://www.compaq.com/easydeploy>.

Altiris eXpress HP/Compaq Client Manager

La herramienta Altiris eXpress HP/Compaq Client Manager integra tecnología Intelligent Manageability de HP en Altiris eXpress para proporcionar capacidades superiores de gestión de hardware para dispositivos de acceso de HP, como por ejemplo:

- Vistas detalladas de inventario de hardware para la gestión de activos
- Diagnóstico y supervisión del funcionamiento del PC
- Notificación proactiva de cambios en el entorno de hardware
- Informes accesibles vía Internet sobre detalles críticos del negocio, tales como máquinas con advertencias térmicas, alertas de memoria, etc.
- Actualización remota del software del sistema, como por ejemplo, controladores de dispositivo y ROM BIOS

Para obtener más información sobre Altiris eXpress HP/Compaq Client Manager, visite <http://www.compaq.com/easydeploy>.

System Software Manager

System Software Manager (SSM) es una utilidad que permite actualizar el software del sistema de varios sistemas simultáneamente. Cuando se ejecuta en un sistema de cliente PC, SSM detecta tanto la versión de hardware como la de software y, a continuación, actualiza el software adecuado desde un repositorio central, también denominado almacén de archivos. Las versiones de controladores que SSM admite se indican mediante un icono especial en la página Web de descargas de controladores y en el CD de software de soporte. Para descargar la utilidad o para obtener más información sobre SSM, visite <http://www.compaq.com/im/ssmwp.html>.

Product Change Notification

Product Change Notification (PCN) es el programa de notificación de cambios en el producto de HP que utiliza una página Web segura en la que se crean perfiles personalizados para, de forma proactiva y automática, poder:

- Recibir notificaciones por correo electrónico de cambios realizados en el hardware y el software de la mayoría de los equipos y servidores comerciales.
- Recibir un correo electrónico que contenga consejos para el cliente respecto a la mayoría de los equipos y servidores comerciales.

La página Web de PCN también permite a los usuarios buscar todas las notificaciones de cambio del producto y consejos para el cliente de la mayoría de los PC y servidores comerciales.

Para saber más sobre PCN y crear su perfil personalizado, visite <http://www.compaq.com/pcn>.

ActiveUpdate

ActiveUpdate es una aplicación basada en el cliente de HP. El cliente ActiveUpdate funciona en el sistema local y utiliza el perfil definido por el usuario para descargar de forma proactiva y automática actualizaciones de software para la mayoría de los equipos y servidores comerciales de Compaq/HP.

Para saber más sobre ActiveUpdate, descargar la aplicación y crear un perfil personalizado, visite

<http://www.compaq.com/activeupdate>.

Memoria flash de la ROM

El equipo se entrega con una memoria flash de la ROM reprogramable. Es posible establecer una contraseña de configuración en la utilidad Computer Setup (F10) para proteger la ROM ante actualizaciones o sobrescrituras inadvertidas. Esto es importante para garantizar la integridad operativa del equipo. Si necesita o desea actualizar la ROM, puede:

- Solicitar un disquete *ROMPaq*™ actualizado de HP.
- Descargar las últimas imágenes de ROMPaq de <http://www.compaq.com>.



PRECAUCIÓN: Para garantizar una protección máxima de la ROM, asegúrese de establecer una contraseña de configuración. La contraseña de configuración impide cualquier actualización de la ROM no autorizada. System Software Manager permite al administrador del sistema establecer la contraseña de configuración en uno o más ordenadores de forma simultánea. Para obtener más información, visite <http://www.compaq.com/im/ssmwp.html>.

Memoria flash de la ROM remota

Gracias a la memoria flash de la ROM remota, el administrador del sistema puede actualizar de forma segura la memoria ROM de equipos HP remotos desde la consola de gestión de red centralizada. Al permitir al administrador del sistema realizar esta tarea de forma remota en varios equipos y PC, se consigue una distribución coherente y un mayor control de las imágenes de la memoria ROM de PC de HP en toda la red. También se logra una mayor productividad y un menor coste total de propiedad.



El equipo debe estar encendido, o en estado de activación remota, para poder aprovechar la memoria flash de la ROM remota.

Para obtener más información sobre la memoria flash de la ROM remota, consulte Altiris eXpress HP/Compaq Client Manager o System Software Manager en <http://www.compaq.com/easydeploy>.

FailSafe Boot Block ROM

La herramienta FailSafe Boot Block ROM permite la recuperación del sistema en el caso improbable de que se produjera un fallo de la memoria flash de la ROM, como por ejemplo, un fallo de alimentación durante la actualización de la ROM. El bloque de arranque es una sección protegida de la memoria flash de la ROM que comprueba si existe una memoria flash válida cuando se enciende el sistema.

- Si la ROM del sistema es válida, el sistema se inicia normalmente.
- Si la ROM del sistema no pasa la comprobación de validación, FailSafe Boot Block ROM proporcionará soporte suficiente para iniciar el sistema desde un disquete ROMPaq, que programará la ROM del sistema con una imagen válida.

Cuando el bloque de arranque detecta una ROM que no es válida, el sistema emite una serie de pitidos (uno largo y tres cortos) y los tres indicadores luminosos del teclado parpadean (se apagan y se encienden dos veces). Se visualizará un mensaje del modo de recuperación de bloque de arranque en la pantalla (determinados modelos).

Para recuperar el sistema cuando se encuentra en modo de recuperación de bloque de arranque, siga los pasos siguientes:


1. Extraiga cualquier disquete de la unidad de disquete y apague el equipo.
2. Inserte un disquete ROMPaq en la unidad correspondiente.
3. Vuelva a encender el sistema.
4. Si el sistema no detecta ningún disquete ROMPaq, le solicitará que inserte uno y reinicie el equipo.
5. Si ha establecido una contraseña de configuración, el indicador luminoso Bloq Mayús se encenderá y el sistema solicitará que introduzca la contraseña.
6. Introduzca la contraseña de configuración.
7. Si el sistema se inicia satisfactoriamente desde el disquete y vuelve a programar la ROM, se encenderán los tres indicadores luminosos del teclado. Una serie de tonos ascendentes indican también que la finalización ha sido correcta.

Para verificar que la memoria flash de la ROM ha sido satisfactoria, siga estos pasos:

1. Inserte un disquete ROMPaq válido en la unidad correspondiente.
2. Apague el sistema.
3. Encienda el sistema para volver a crear una memoria flash de la ROM.
4. Si la memoria flash de la ROM es satisfactoria, los tres indicadores luminosos del teclado se encenderán y podrá oír una serie de pitidos en tono ascendente.
5. Extraiga el disquete, apague el equipo y, a continuación, vuelva a iniciarlo.

En la tabla siguiente se enumeran las diversas combinaciones de indicadores luminosos del teclado utilizadas por la ROM de bloque de arranque, así como el significado y la acción asociada con cada combinación.

Combinaciones de indicadores luminosos del teclado utilizadas por la ROM de bloque de arranque

Modo de bloque de arranque de seguridad	Color del indicador luminoso del teclado	teclado Actividad de los indicadores luminosos	Estado/Mensaje
Bloq Num	Verde	Encendido	Disquete ROMPaq no presente, defectuoso o unidad no preparada.*
Bloq Mayús	Verde	Encendido	Introduzca la contraseña.*
Bloq Num, Bloq Mayús, Bloq Despl	Verde	Se enciende y se apaga 2 veces (junto con 1 pitido largo y 3 cortos)	Fallo de la memoria flash de la ROM.*
Bloq Num, Bloq Mayús, Bloq Despl	Verde	Encendido	Boot Block de la memoria flash de la ROM satisfactorio. Apagar y, a continuación, volver a arrancar.
 Los indicadores luminosos de diagnóstico no parpadean en los teclados USB.			

Replicación de la configuración

Este procedimiento permite al administrador copiar fácilmente una configuración en otros equipos del mismo modelo. Esto facilita la configuración rápida y más coherente de varios equipos. Para replicar la configuración:

1. Acceda al menú de utilidades de Computer Setup (F10).
2. Haga clic en **File (Archivo) > Save to Diskette (Guardar en disquete)**. Siga las instrucciones de la pantalla.



Esto requiere una unidad de disquete interna o una unidad de disquete externa, portátil.

3. Para replicar la configuración, haga clic en **File (Archivo) > Restore from Diskette (Restaurar desde disquete)** y siga las instrucciones de la pantalla.

Altiris eXpress, System Software Manager y PC Transplant hacen que resulte fácil replicar la configuración y valores personalizados de un ordenador y copiarlos a uno o más ordenadores. Para obtener más información, visite <http://www.compaq.com/easydeploy>.

Botón de alimentación de modo dual

Si la interfaz ACPI (interfaz de alimentación y configuración avanzada) está activada para Windows 98, Windows 2000, Windows Millennium y Windows XP, el botón de alimentación puede funcionar como botón de encendido o de apagado o bien como botón de suspensión. La función de suspensión no apaga completamente el equipo, sino que hace que entre en modo de estado de espera de bajo consumo. Esto permite apagar rápidamente el sistema sin tener que cerrar las aplicaciones y volver rápidamente al mismo estado operativo en que se encontraba sin que se produzcan pérdidas de datos.

Para cambiar la configuración del botón de alimentación, siga estos pasos:

1. En Windows 2000, haga clic con el botón de la izquierda en **Inicio**, seleccione **Configuración > Panel de control > Opciones de energía**.
En Windows XP, haga clic con el botón de la izquierda en **Inicio**, seleccione **Panel de control > Rendimiento y mantenimiento > Opciones de energía**.
2. En **Propiedades de Opciones de energía**, seleccione la pestaña **Opciones Avanzadas**.
3. En la sección Botones de encendido, seleccione la configuración de botón de encendido deseada.

Tras configurar el botón de alimentación para que funcione como un botón de suspensión, pulse el botón de alimentación para que el sistema pase al estado de ahorro de energía (suspendido). Pulse el botón de nuevo para que el sistema pase rápidamente al estado normal de funcionamiento. Para apagar completamente el sistema, mantenga pulsado el botón de alimentación durante cuatro segundos.

Power Management

Power Management es una función que cierra determinados componentes del equipo cuando no se utilizan, lo que permite ahorrar energía sin tener que apagar el equipo.

Si la interfaz ACPI (Interfaz de alimentación y configuración avanzada) está activada para Windows 98, Windows 2000, Windows Millennium y Windows XP, los tiempos de espera (el periodo de inactividad permitido antes de cerrar estos componentes) se pueden activar, personalizar o desactivar con el sistema operativo.

1. En Windows 2000, haga clic con el botón de la izquierda en **Inicio**, seleccione **Configuración > Panel de control > Opciones de energía**.

En Windows XP, haga clic con el botón de la izquierda en **Inicio**, seleccione **Panel de control > Rendimiento y mantenimiento > Opciones de energía**.

2. En **Propiedades de Opciones de energía**, seleccione la pestaña **Combinaciones de energía**.
3. Seleccione la configuración de combinación de energía deseada.

Utilice las propiedades de la pantalla para establecer, modificar o desactivar los valores de gestión de energía del monitor. Para acceder a Propiedades de pantalla, haga clic con el botón derecho del ratón en el **escritorio de Windows** y seleccione **Propiedades**.

Página Web

Los ingenieros de HP prueban de forma rigurosa y depuran el software desarrollado por HP y otros fabricantes, y desarrollan software de soporte específico para el sistema operativo a fin de garantizar el nivel de rendimiento, compatibilidad y fiabilidad más elevado en los equipos de HP.

Cuando se realiza la transición a sistemas operativos nuevos o revisados, es importante implementar el software de soporte diseñado para el sistema operativo en cuestión. Si planea ejecutar una versión de Microsoft Windows que no sea la versión incluida con el equipo, deberá instalar los controladores de dispositivo y las utilidades correspondientes para garantizar la compatibilidad y el funcionamiento adecuado de todas las características.

HP ha facilitado la tarea de localizar, acceder, evaluar e instalar el software de soporte más reciente. Puede descargar el software de <http://www.compaq.com>.

La página Web contiene los controladores de dispositivo, las utilidades y las imágenes de la memoria flash de la ROM más actuales necesarios para ejecutar el sistema operativo Microsoft Windows más reciente en el equipo HP.

Productos base y empresas colaboradoras

Las soluciones de gestión de HP se basan en los estándares de la industria, incluidas las tecnologías DMI 2.0, Web-Based Enterprise Management, Wired for Management (WfM) de Intel, SNMP y PXE (Preboot Execution Environment). Microsoft, Intel, Altiris y otras empresas líderes del sector trabajan junto con HP para integrar sus soluciones de gestión con los productos e iniciativas de HP para proporcionar a los clientes de HP las soluciones más actuales de Intelligent Manageability para sistemas personales. Para obtener más información, visite <http://www.compaq.com/easydeploy>.

Desktop Management Interface (DMI)

Desktop Management Task Force (DMTF) es un organismo de la industria creado en 1992 con el objetivo de estandarizar la manejabilidad de sistemas. DMTF estableció la estructura de la DMI para estandarizar el acceso a los datos de configuración del PC. HP, como miembro del comité de dirección y el comité técnico de DMTF, proporciona instrumentos de hardware y software que admiten el estándar DMI.

Para obtener más información sobre la configuración del software DMI, consulte el archivo de ayuda *Intelligent Manageability Guide* (*Guía de Intelligent Manageability*).

Wired for Management

La iniciativa Wired for Management de Intel se centra en la reducción del coste de soporte y administración de los sistemas basados en arquitectura de Intel sin comprometer la flexibilidad y el rendimiento. Las directrices Wired for Management proporcionan un conjunto de productos base que HP utiliza en Intelligent Manageability para proporcionar gestión estandarizada de inventarios de equipos de sobremesa, configuración remota del sistema, mantenimiento fuera del horario de trabajo y gestión de la alimentación de generación futura. Pero HP no se limita a estas funciones básicas. Se han incorporado capacidades adicionales en Intelligent Manageability para proporcionar una solución exhaustiva para gestionar entornos de equipos conectados a redes.

Las tecnologías Wired for Management incluyen:

- Desktop Management Interface (DMI) 2.0
- Remote System Installation
- Activación remota y cierre remoto
- Hardware compatible con ACPI
- SMBIOS
- Soporte de ejecución previa al arranque (PXE)

Seguimiento y seguridad de activos

Las funciones AssetControl de Compaq incorporadas en el equipo proporcionan datos de seguimiento de activos clave que pueden gestionarse mediante los productos de HP Insight Manager y de Management Solutions Partners. La integración automática y transparente entre las funciones AssetControl y dichos productos permite seleccionar la herramienta de gestión que mejor se adapta al entorno y aprovechar la inversión realizada en las herramientas de las que ya se dispone.

Los equipos HP se fabrican con el hardware y firmware necesario para que sean totalmente compatibles con el estándar DMI 2.0.

HP también ofrece varias soluciones para controlar el acceso a componentes e información valiosos. Las características de seguridad, como por ejemplo, el sensor de Smart Cover y el bloqueo de Smart Cover, disponibles en determinados modelos, ayudan a impedir el acceso no autorizado a los componentes internos del equipo. Para proteger los activos de datos valiosos, desactive los puertos paralelo, serie o USB, o bien las capacidades de arranque de soporte extraíble. Las alertas de cambio de memoria y del sensor de Smart Cover pueden enviarse automáticamente a los productos de HP Insight Manager para entregar una notificación proactiva de que se están manipulando los componentes internos del equipo.



El sensor de Smart Cover y el bloqueo de Smart Cover están disponibles como opciones en determinados sistemas.

Utilice las utilidades siguientes para gestionar valores de seguridad en el equipo de HP:

- De forma local, mediante las utilidades de Computer Setup. Para obtener información adicional e instrucciones sobre cómo utilizar las utilidades de Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)* que se entrega con el equipo.
- De forma remota, mediante System Software Manager. Este software permite distribuir, de forma segura y coherente, y controlar los valores de seguridad de una utilidad simple de la línea de comandos.

La tabla y los apartados siguientes hacen referencia a la gestión de características de seguridad del equipo, de forma local, mediante las utilidades de Computer Setup (F10).

Descripción general de las características de seguridad

Elemento	Objetivo	Cómo se establece
Control de arranque desde soporte extraíble	Impedir el arranque desde unidades de soporte extraíbles.	Desde el menú de utilidades de Computer Setup (F10).
Control de las interfaces serie, paralela, USB o de infrarrojos	Impedir la transferencia de datos a través de las interfaces integradas serie, paralela, USB o de infrarrojos.	Desde el menú de utilidades de Computer Setup (F10).
Power-On Password (Contraseña de arranque)	Impedir que se utilice el equipo si no se ha introducido la contraseña. Esto es válido tanto para el arranque inicial del sistema como para cualquier reinicio.	Desde el menú de utilidades de Computer Setup (F10).
Setup Password (Contraseña de configuración)	Impedir que se modifique la configuración del equipo (uso de las utilidades de Computer Setup) si no se ha introducido la contraseña.	Desde el menú de utilidades de Computer Setup (F10).
Modo de servidor de red	Proporcionar características de seguridad únicas para equipos que se utilizan como servidores.	Desde el menú de utilidades de Computer Setup (F10).
DriveLock (Bloqueo de la unidad)	Impedir el acceso no autorizado a los datos en unidades de disco duro específicas. Esta función sólo está disponible en determinados modelos.	Desde el menú de utilidades de Computer Setup (F10).

Descripción general de las características de seguridad (continuación)

Elemento	Objetivo	Cómo se establece
Sensor de Smart Cover	Indicar que se ha extraído la cubierta o el panel lateral del equipo. Se puede hacer que solicite la contraseña de configuración para reiniciar el equipo, una vez extraída la cubierta o el panel lateral. Para obtener más información sobre esta función, consulte la publicación <i>Guía de referencia del hardware</i> en el CD <i>Biblioteca de documentación</i> .	Desde el menú de utilidades de Computer Setup (F10).
Master Boot Record Security (Seguridad del registro de arranque maestro)	Impedir que se efectúen cambios no intencionados o maliciosos en el registro maestro del disco de arranque actual, y proporciona un medio para recuperar el último registro maestro de arranque correcto.	Desde el menú de utilidades de Computer Setup (F10).
Alertas de cambio de memoria	Detectar si se han añadido, movido o extraído módulos de memoria, y notificar estos cambios al usuario y al administrador del sistema.	Para obtener más información sobre cómo activar las alertas de cambio de memoria, consulte la publicación en línea <i>Intelligent Manageability Guide</i> (Guía de Intelligent Manageability).
Identificador de propiedad	Mostrar la información de propiedad, según la definición del administrador del sistema, al arrancar el sistema (protegido por la contraseña de configuración).	Desde el menú de utilidades de Computer Setup (F10).

Descripción general de las características de seguridad (continuación)

Elemento	Objetivo	Cómo se establece
Candado con cadena	Inhibir el acceso al interior del equipo para impedir cambios de configuración no deseados o la extracción de componentes. También se puede utilizar para fijar el equipo a un elemento fijo a fin de impedir un posible robo.	Instale una cadena para fijar el equipo a un elemento fijo.
Bucle de seguridad	Inhibir el acceso al interior del equipo para impedir cambios de configuración no deseados o la extracción de componentes.	Instale un candado en el bucle de seguridad para impedir cambios de configuración no deseados o la extracción de componentes.



Para obtener más información sobre Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)*.

Las características de seguridad admitidas pueden variar según la configuración específica del equipo.

Seguridad mediante contraseña

La contraseña de arranque impide la utilización no autorizada del equipo ya que se solicita la introducción de una contraseña para acceder a aplicaciones o a datos cada vez que se enciende o reinicia el equipo. La contraseña de configuración impide específicamente el acceso no autorizado a Computer Setup, y también se puede utilizar en sustitución de la contraseña de arranque. Es decir, si cuando se solicita la contraseña de arranque se introduce en su lugar la contraseña de configuración, se podrá acceder igualmente al equipo.

Se puede establecer una contraseña de configuración de toda la red para que el administrador del sistema pueda conectarse a todos los sistemas de la red y realizar tareas de mantenimiento sin necesidad de conocer la contraseña de arranque, aunque se haya definido una.

Definición de una contraseña de configuración mediante Computer Setup

La definición de una contraseña de configuración mediante Computer Setup evita tener que configurar de nuevo el equipo (uso de la utilidad de Computer Setup (F10)) hasta que se haya introducido la contraseña.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el indicador Computer Setup en la esquina inferior derecha de la pantalla, pulse la tecla **F10**. Pulse **Enter** para omitir la pantalla de título, si procede.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Seleccione **Security (Seguridad)** y, a continuación, **Setup Password (Contraseña de configuración)**, y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **File (Archivo) > Save Changes and Exit (Guardar cambios y salir)**.

Definición de una contraseña de arranque mediante Computer Setup

La definición de una contraseña de arranque mediante Computer Setup impide el acceso al equipo cuando está encendido si no se introduce la contraseña. Si se ha establecido una contraseña de arranque, podrá seleccionar Password Options (Opciones de contraseña) en el menú Security (Seguridad) de Computer Setup. Las opciones de contraseña son Network Server Mode (Modo de servidor de red) y Password Prompt on Warm Boot (Solicitud de contraseña durante un arranque en caliente).

Si se ha desactivado el modo de servidor de red, la contraseña debe introducirse cada vez que al encender el equipo aparece el icono de llave en la pantalla. Si se ha activado la solicitud de contraseña durante un arranque en caliente, la contraseña también debe introducirse cada vez que se reinicia el equipo. Si se ha activado el modo de servidor de red, durante la POST no se solicitará la contraseña, pero cualquier teclado PS/2 conectado permanecerá bloqueado hasta que el usuario introduzca la contraseña de arranque.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el indicador Computer Setup en la esquina inferior derecha de la pantalla, pulse la tecla **F10**. Pulse **Enter** para omitir la pantalla de título, si procede.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Seleccione **Security (Seguridad)** y, a continuación, **Power-On Password (Contraseña de arranque)**, y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **File (Archivo) > Save Changes and Exit (Guardar cambios y salir)**.

Introducción de una contraseña de arranque

Para introducir una contraseña de arranque, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el icono de llave en la pantalla, escriba la contraseña actual y, a continuación, pulse **Enter**.



Preste atención al escribir la contraseña, puesto que por motivos de seguridad los caracteres que se escriben no aparecen en la pantalla.

Si la contraseña introducida no es correcta, aparecerá un icono de llave rota. Inténtelo de nuevo. Al cabo de tres intentos sin éxito, deberá apagar el equipo y volver a encenderlo para poder continuar.

Introducción de una contraseña de configuración

Si se ha establecido una contraseña de configuración en el equipo, ésta se solicitará cada vez que se ejecute Computer Setup.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el mensaje F10 = Setup (F1 = Configuración) en la esquina inferior derecha de la pantalla, pulse la tecla **F10**.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Cuando aparezca el icono de llave en la pantalla, escriba la contraseña de configuración y, a continuación, pulse la tecla **Enter**.



Preste atención al escribir la contraseña, puesto que por motivos de seguridad los caracteres que se escriben no aparecen en la pantalla.

Si la contraseña introducida no es correcta, aparecerá un icono de llave rota. Inténtelo de nuevo. Al cabo de tres intentos sin éxito, deberá apagar el equipo y volver a encenderlo para poder continuar.

Modificación de una contraseña de arranque o de configuración

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**. Para modificar la contraseña de configuración, ejecute **Computer Setup**.
2. Cuando aparezca el icono de llave, escriba la contraseña actual, una barra inclinada (/) o un carácter delimitador alternativo, la nueva contraseña, otra barra inclinada (/) o un carácter delimitador alternativo, y otra vez la nueva contraseña, tal como se indica a continuación: **contraseña actual/nueva contraseña/nueva contraseña**



Preste atención al escribir la contraseña, puesto que por motivos de seguridad los caracteres que se escriben no aparecen en la pantalla.

3. Pulse la tecla **Enter**.

La nueva contraseña se aplicará la próxima vez que encienda el equipo.



Para obtener información acerca de los caracteres delimitadores alternativos, consulte el apartado “Caracteres delimitadores de un teclado nacional” de este capítulo. La contraseña de arranque y la contraseña de configuración también pueden modificarse mediante las opciones de seguridad de Computer Setup.

Eliminación de una contraseña de arranque o de configuración

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**. Para eliminar la contraseña de configuración, ejecute **Computer Setup**.
2. Cuando aparezca el icono de llave, escriba la contraseña actual seguida de una barra inclinada (/) o un carácter delimitador alternativo, tal como se muestra a continuación:
contraseña actual/
3. Pulse la tecla **Enter**.



Para obtener información acerca de los caracteres delimitadores alternativos, consulte el apartado “Caracteres delimitadores de un teclado nacional”. La contraseña de arranque y la contraseña de configuración también pueden modificarse mediante las opciones de seguridad de Computer Setup.

Caracteres delimitadores de un teclado nacional

Los distintos teclados se diseñan conforme a los requisitos específicos de cada país. La sintaxis y las teclas que cada usuario utiliza para modificar o eliminar la contraseña dependen del teclado que se entregó con el equipo.

Caracteres delimitadores de un teclado nacional

Árabe	/	Griego	–	Ruso	/
Belga	=	Hebreo	–	Eslovaco	–
BHCEY*	–	Húngaro	–	Español	–
Brasileño	/	Italiano	–	Sueco/Finlandés	/
Chino	/	Japonés	/	Suizo	–
Checo	–	Coreano	/	Taiwanés	/
Danés	–	Latinoamericano	–	Tailandés	/
Francés	!	Noruego	–	Turco	–
Francés canadiense	é	Polaco	–	Inglés británico	/

*Para Bosnia-Herzegovina, Croacia, Eslovenia y Yugoslavia

Cómo borrar contraseñas

Si olvida la contraseña, no podrá acceder al equipo. Para obtener instrucciones acerca de cómo borrar contraseñas, consulte la *Guía de solución de problemas*.

Modo de servidor de red

El modo de servidor de red proporciona características de seguridad únicas para equipos que se utilizan como servidores. Sólo está disponible si se ha establecido una contraseña de arranque en Computer Setup. Si se ha activado el modo de servidor de red, no es necesario utilizar la contraseña de arranque para arrancar la unidad de disco duro, ni tampoco que haya un teclado conectado al sistema. En el caso de que haya un teclado PS/2 conectado, éste se bloqueará hasta que el usuario introduzca la contraseña de arranque. En el caso de que haya un teclado USB conectado, éste permanecerá activo de forma predeterminada. Para impedir el acceso mediante el teclado USB una vez cargado el sistema operativo, un usuario debe ocultar el puerto USB en la opción Device Security (Seguridad de dispositivos) del menú Security (Seguridad) de Computer Setup. Cuando se utiliza conjuntamente con la opción de arranque After Power Loss (Tras un corte de alimentación) de Computer Setup, el modo de servidor de red permite al “servidor” volver a arrancar automáticamente tras un corte de alimentación sin necesidad de que intervenga el usuario. Si se ha establecido el modo de servidor de red, la contraseña de arranque debe introducirse para arrancar los soportes extraíbles (por ejemplo, disquetes) o los dispositivos extraíbles (por ejemplo, dispositivos flash USB).

DriveLock (Bloqueo de la unidad)

El bloqueo de la unidad es una característica de seguridad que impide el acceso no autorizado a los datos de determinadas unidades de disco duro. Esta función se ha implementado como una extensión de Computer Setup. Sólo está disponible en determinados sistemas y únicamente cuando se detectan unidades de disco duro que admiten el bloqueo de la unidad.

La función de bloqueo de la unidad ha sido ideada para los clientes de HP cuya preocupación principal es la seguridad de los datos. Para dichos clientes, el coste de la unidad de disco duro y la pérdida de los datos almacenados en ésta es irrelevante en comparación con los daños que pueden resultar del acceso no autorizado al contenido. A fin de equilibrar este nivel de seguridad con la necesidad práctica de facilitar una contraseña olvidada, el bloqueo de la unidad utiliza un esquema de seguridad de dos contraseñas. El administrador del sistema establece y utiliza una de las contraseñas, mientras que la otra la establece y utiliza normalmente el usuario final. La unidad no puede desbloquearse si se han olvidado ambas contraseñas. Por lo tanto, la forma más segura de utilizar el bloqueo de la unidad es duplicar los datos de la unidad de disco duro en un sistema de información corporativo o hacer una copia de seguridad periódicamente.

En el caso de que se pierdan ambas contraseñas de bloqueo, la unidad de disco duro queda inutilizada. Para los usuarios que no se ajustan al perfil de cliente anteriormente definido, esto puede suponer un riesgo inaceptable. Para los usuarios que se ajustan al perfil del cliente, puede existir un riesgo tolerable dada la naturaleza de los datos almacenados en la unidad de disco duro.

Utilización de la opción de bloqueo de la unidad

La opción DriveLock (bloqueo de la unidad) aparece en el menú Security (Seguridad) de Computer Setup. El usuario tiene la posibilidad de establecer la contraseña maestra o de activar el bloqueo de la unidad. Debe proporcionarse una contraseña de usuario para activar el bloqueo de la unidad. Dado que la configuración inicial del bloqueo de la unidad la realiza normalmente un administrador del sistema, primero debe establecerse una contraseña maestra. HP recomienda a los administradores del sistema que establezcan una contraseña maestra tanto si desean activar el bloqueo de la unidad como si lo dejan desactivado. De esta manera, el administrador tiene la posibilidad de modificar los valores de bloqueo de la unidad en el caso de que posteriormente se active esta función. Una vez establecida la contraseña maestra, el administrador del sistema puede activar el bloqueo de la unidad o dejarlo desactivado.

En el caso de una unidad de disco duro bloqueada, la POST solicitará una contraseña para desbloquear el dispositivo. Si se ha establecido una contraseña de arranque que coincide con la contraseña de usuario del dispositivo, la POST no solicitará que se vuelva a introducir la contraseña. De lo contrario, el usuario deberá introducir una contraseña de bloqueo de la unidad. Puede utilizarse tanto la contraseña maestra como la contraseña de usuario. Los usuarios dispondrán de dos intentos para introducir una contraseña correcta. Si ninguno tiene éxito, la POST continuará pero no se podrá acceder a los datos de la unidad.

Aplicaciones de bloqueo de la unidad

La utilización más práctica de la característica de seguridad de bloqueo de la unidad es en un entorno corporativo en el que un administrador del sistema proporciona unidades de disco duro para el compartimiento multiusuario a los usuarios para que las utilicen en determinados equipos. El administrador del sistema será el responsable de configurar la unidad de disco duro para el compartimiento multiusuario que implicará, entre otras cosas, establecer la contraseña maestra del bloqueo de la unidad. En el caso de que el usuario olvide su contraseña o que otro empleado utilice el equipo, siempre puede utilizarse la contraseña maestra para volver a establecer la contraseña de usuario y tener nuevamente acceso a la unidad de disco duro.

HP recomienda a los administradores de sistemas corporativos que optan por activar el bloqueo de la unidad que establezcan también una política corporativa para establecer y mantener las contraseñas maestras. Esto debe realizarse para evitar una situación en que un empleado modifique de forma intencionada o no ambas contraseñas de bloqueo de la unidad antes de abandonar la compañía. En tal caso, la unidad de disco duro quedaría inutilizada y debería reemplazarse. Asimismo, si no se establece una contraseña maestra, los administradores del sistema pueden encontrarse con el acceso bloqueado a una unidad de disco duro, sin posibilidad de realizar comprobaciones de rutina para detectar software no autorizado, ni otras funciones de control de activos y soporte técnico.

Para los usuarios con requisitos de seguridad menos estrictos, HP no recomienda que se active el bloqueo de la unidad. Entre los usuarios de esta categoría se incluyen los usuarios particulares o los usuarios que no mantienen datos sensibles en las unidades de disco duro de forma habitual. Para estos usuarios, la pérdida potencial de una unidad de disco duro consecuencia del olvido de ambas contraseñas es más importante que el valor de los datos para los que se ha diseñado la función de bloqueo de la unidad. Puede restringirse el acceso a Computer Setup y DriveLock mediante la contraseña de configuración. Al especificar una contraseña de configuración y no proporcionarla a los usuarios finales, los administradores del sistema restringen los usuarios que pueden activar el bloqueo de la unidad.

Sensor de Smart Cover

El sensor de Smart Cover, disponible en determinados modelos, es una combinación de tecnología de hardware y de software que permite recibir alertas en el caso de que se extraiga la cubierta o el panel lateral del equipo. Existen tres niveles de protección, descritas en la tabla siguiente.

Niveles de protección del sensor de Smart Cover

Nivel	Valor	Descripción
Nivel 0	Disabled (Desactivado)	Sensor de Smart Cover desactivado (valor predeterminado).
Nivel 1	Notify User (Notificar al usuario)	Cuando se reinicia el equipo, la pantalla visualiza un mensaje en el que se indica que se ha extraído la cubierta o el panel lateral del equipo.
Nivel 2	Setup Password (Contraseña de configuración)	Cuando se reinicia el equipo, la pantalla visualiza un mensaje en el que se indica que se ha extraído la cubierta o el panel lateral del equipo. Debe introducir la contraseña de configuración para poder continuar.



Estos valores pueden modificarse mediante Computer Setup. Para obtener más información sobre Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)*.

Configuración del nivel de protección del sensor de Smart Cover

Para establecer el nivel de protección del sensor de Smart Cover, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el indicador Computer Setup en la esquina inferior derecha de la pantalla, pulse la tecla **F10**. Pulse **Enter** para omitir la pantalla de título, si procede.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Seleccione **Security (Seguridad)** y, a continuación, **Smart Cover (Cubierta inteligente)**, y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **File (Archivo) > Save Changes and Exit (Guardar cambios y salir)**.

Bloqueo de Smart Cover

El bloqueo de Smart Cover es un bloqueo de la cubierta controlable por software que incorporan determinados equipos de HP. Este bloqueo impide el acceso no autorizado a los componentes internos. Los equipos se entregan con la función de bloqueo de Smart Cover en la posición de desbloqueo.



PRECAUCIÓN: Para garantizar una seguridad máxima del bloqueo de la cubierta, asegúrese de establecer una contraseña de configuración. La contraseña de configuración impide el acceso no autorizado a la utilidad de Computer Setup.



El bloqueo de Smart Cover está disponible como opción en determinados sistemas.

Activación del bloqueo de Smart Cover

Para activar el bloqueo de Smart Cover, siga los pasos siguientes:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el indicador Computer Setup en la esquina inferior derecha de la pantalla, pulse la tecla **F10**. Pulse **Enter** para omitir la pantalla de título, si procede.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Seleccione **Security (Seguridad)** y, a continuación, seleccione **Smart Cover (Cubierta inteligente)** y la opción **Locked (Bloqueado)**.
4. Antes de salir, haga clic en **File (Archivo) > Save Changes and Exit (Guardar cambios y salir)**.

Desactivación del bloqueo de Smart Cover

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el indicador Computer Setup en la esquina inferior derecha de la pantalla, pulse la tecla **F10**. Pulse **Enter** para omitir la pantalla de título, si procede.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Seleccione **Security (Seguridad) > Smart Cover (Cubierta inteligente) > Unlocked (Desbloqueado)**.
4. Antes de salir, haga clic en **File (Archivo) > Save Changes and Exit (Guardar cambios y salir)**.

Utilización de la llave de seguridad de Smart Cover

Si activa el bloqueo Smart Cover y no puede escribir la contraseña para desactivar el bloqueo, necesitará la llave de seguridad Smart Cover para abrir la cubierta del equipo. Necesitará la llave en cualquiera de las circunstancias siguientes:

- Corte de alimentación
- Fallo de arranque
- Fallo de un componente de PC (por ejemplo, procesador o fuente de alimentación)
- Olvido de la contraseña



PRECAUCIÓN: La llave de seguridad de Smart Cover es una herramienta especializada de HP. Esté preparado; pida esta llave antes de que necesite una en un distribuidor o proveedor de servicios autorizado (pida el n° de pieza 166527-001 para la llave de tipo llave inglesa o el n° de pieza 166527-002 para la llave de tipo destornillador).

Para obtener la llave de seguridad, siga uno de los pasos siguientes:

- Póngase en contacto con su distribuidor o el servicio técnico autorizado de HP.
- Visite <http://www.compaq.com> para la información de pedido.
- Llame al número correspondiente que se indica en la garantía.

Para obtener más información sobre como utilizar la llave de seguridad de Smart Cover, consulte la publicación *Guía de referencia del hardware*.

Master Boot Record Security (Seguridad del registro de arranque maestro)

El registro de arranque maestro contiene información necesaria para arrancar correctamente un disco y acceder a los datos almacenados en el mismo. La seguridad del registro de arranque maestro puede impedir cambios inadvertidos o maliciosos en el registro de arranque maestro, tales como los provocados por ciertos virus informáticos o por el uso incorrecto de determinadas utilidades de disco. También permite recuperar el último registro de arranque maestro correcto, si se detectan cambios en dicho registro cuando se reinicia el sistema.

Para activar la seguridad del registro de arranque maestro, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el indicador Computer Setup en la esquina inferior derecha de la pantalla, pulse la tecla **F10**. Pulse **Enter** para omitir la pantalla de título, si procede.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Seleccione **Security (Seguridad) > Master Boot Record Security (Seguridad del registro de arranque maestro) > Enabled (Activado)**.
4. Seleccione **Security (Seguridad) > Save Master Boot Record (Guardar registro de arranque maestro)**.
5. Antes de salir, haga clic en **File (Archivo) > Save Changes and Exit (Guardar cambios y salir)**.

Si se ha activado la seguridad del registro de arranque maestro, el BIOS impide que se efectúen cambios en el registro de arranque maestro del disco de arranque actual cuando se trabaja en el modo de seguridad de MS-DOS o Windows.



La mayoría de los sistemas operativos controlan el acceso al registro de arranque maestro del disco de arranque actual; el BIOS no puede impedir que se efectúen cambios cuando se está ejecutando el sistema operativo.

Cada vez que se enciende o se reinicia el equipo, el BIOS compara el registro de arranque maestro del disco de arranque actual con el registro anteriormente guardado. Si se detectan cambios o si el disco de arranque actual es el disco cuyo registro de arranque maestro se guardó anteriormente, aparecerá un mensaje parecido al siguiente:

1999–Se ha modificado el registro maestro de arranque.

Pulse cualquier tecla para acceder a la utilidad de configuración y configurar la seguridad del registro de arranque maestro.

Tras acceder a Computer Setup, debe:

- Guardar el registro de arranque maestro del disco de arranque actual,
- Restaurar el registro de arranque maestro guardado anteriormente, o bien
- Desactivar la característica de seguridad del registro de arranque maestro.

Debe conocer la contraseña de configuración, en el caso de que exista alguna.

Si se detectan cambios o si el disco de arranque actual **no** es el disco cuyo registro de arranque maestro se guardó anteriormente, aparecerá un mensaje parecido al siguiente:

2000–Se ha modificado el registro maestro de arranque de la unidad de disco duro.

Pulse cualquier tecla para acceder a la utilidad de configuración y configurar la seguridad del registro de arranque maestro.

Tras acceder a Computer Setup, debe:

- Guardar el registro de arranque maestro del disco de arranque actual o bien
- Desactivar la característica de seguridad del registro de arranque maestro.

Debe conocer la contraseña de configuración, en el caso de que exista alguna.

En el caso improbable de que el registro de arranque maestro guardado previamente esté dañado, aparecerá un mensaje parecido al siguiente:

1998–Se ha perdido el registro de arranque maestro.

Pulse cualquier tecla para acceder a la utilidad de configuración y configurar la seguridad del registro de arranque maestro.

Tras acceder a Computer Setup, debe:

- Guardar el registro de arranque maestro del disco de arranque actual o bien
- Desactivar la característica de seguridad del registro de arranque maestro.

Debe conocer la contraseña de configuración, en el caso de que exista alguna.

Antes de crear una partición del disco de arranque actual o formatearlo

Asegúrese de que se ha desactivado la seguridad del registro de arranque maestro antes de modificar las particiones del disco de arranque actual o dar formato a dicho disco. Algunas utilidades de disco, tales como FDISK y FORMAT, intentan actualizar el registro de arranque maestro. Si la seguridad del registro de arranque maestro está activada cuando modifique la partición o el formato del disco, recibirá mensajes de error de la utilidad de disco o una advertencia de la seguridad del registro de arranque maestro la próxima vez que encienda o reinicie el equipo. Para desactivar la seguridad del registro de arranque maestro, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el indicador Computer Setup en la esquina inferior derecha de la pantalla, pulse la tecla **F10**. Pulse **Enter** para omitir la pantalla de título, si procede.



Si no pulsa la tecla **F10** mientras se visualiza el mensaje, deberá reiniciar el equipo para acceder a la utilidad.

3. Seleccione **Security (Seguridad) > Master Boot Record Security (Seguridad del registro de arranque maestro) > Disabled (Desactivado)**.
4. Antes de salir, haga clic en **File (Archivo) > Save Changes and Exit (Guardar cambios y salir)**.

Candado con cadena

En el panel posterior del equipo hay un candado con cadena para sujetar físicamente el equipo al área de trabajo.

Para obtener instrucciones ilustradas, consulte la publicación *Guía de referencia del hardware* que se encuentra en el CD *Biblioteca de documentación*.

Tecnología de identificación de huellas digitales

Al eliminar la necesidad de introducir contraseñas de usuario, la tecnología de identificación de huellas digitales de HP refuerza la seguridad de la red, simplifica el proceso de conexión y reduce los costes asociados con la gestión de redes corporativas. Esta tecnología, cuyo precio es razonable, ya no está dirigida solamente a organizaciones de alta tecnología y seguridad.



La compatibilidad con la tecnología de identificación de huellas digitales varía según el modelo.

Para obtener más información, visite:

http://www.compaq.com/products/quickspecs/10690_na/10690_na.html

Notificación y recuperación de fallos

Las funciones de notificación y recuperación de fallos combinan tecnología de hardware y de software innovadora para impedir la pérdida de datos críticos y minimizar los períodos de no disponibilidad no planeados.

Cuando se produce un fallo, el equipo visualiza un mensaje de alerta local que contiene una descripción del fallo y las acciones recomendadas. Posteriormente, puede verificar el funcionamiento del sistema actual mediante el agente de Insight Manager de HP. Si el equipo está conectado a una red gestionada por un producto Insight Manager de HP u otros productos de gestión de otras empresas de soluciones de gestión que colaboran con Compaq, el equipo también envía un aviso de fallo a la aplicación de gestión de red.

Sistema de protección de unidades

El sistema de protección de unidades (DPS) es una herramienta de diagnóstico incorporada en las unidades de disco duro que están instaladas en determinados equipos de HP. DPS está diseñado para ayudar a diagnosticar problemas que pueden requerir una sustitución de la unidad de disco duro no cubierta por la garantía.

Cuando se fabrican los equipos de HP, las unidades de disco duro instaladas se someten a prueba mediante DPS y se graba un registro permanente de información clave en la unidad. Cada vez que se ejecuta DPS, los resultados de la prueba se graban en la unidad de disco duro. El proveedor de servicios puede utilizar esta información para ayudar a diagnosticar las condiciones que le han llevado a ejecutar el software DPS. Para obtener instrucciones acerca del uso del sistema de protección de unidades, consulte la *Guía de solución de problemas*.

Seguimiento de la integridad de discos Ultra ATA

El seguimiento de la integridad de discos Ultra ATA permite controlar la integridad de los datos a medida que se transfieren entre una unidad de disco duro Ultra ATA y la lógica del sistema. Si el equipo detecta un número anormal de errores de transmisión, el equipo muestra un mensaje de alerta local con las acciones recomendadas.

Fuente de alimentación con protector de sobretensión

Una fuente de alimentación con protector de sobretensión integrada proporciona mayor fiabilidad cuando el equipo se ve afectado por una sobretensión imprevista de la corriente. Esta fuente de alimentación está diseñada para resistir sobretensiones de hasta 2.000 voltios sin causar períodos de no disponibilidad ni pérdidas de datos en el equipo.

Sensor térmico

El sensor térmico es una función de hardware y de software que controla la temperatura interna del equipo. Esta función muestra un mensaje de advertencia cuando se sobrepasa el rango normal de temperaturas, lo que proporciona tiempo al usuario para emprender una acción antes de que se produzcan daños en los componentes internos o pérdidas de datos.

Índice

A

acceso al equipo, controlar 14
ActiveUpdate 6
Altiris eXpress 3
Altiris eXpress HP/Compaq Client
Manager 5
Altiris eXpress PC Transplant Pro 5
AssetControl 14

B

disco de arranque, información importante 31

C

candado con cadena 31
precauciones
 seguridad de bloqueo de la cubierta 26
 llave de seguridad 28
 proteger la ROM 7
cambiar sistemas operativos, información
 importante 12
modificar contraseña 20
borrar contraseña 22
herramientas de clonación, software 2
utilidades de Computer Setup 10
configurar el botón de alimentación 10
controlar el acceso al equipo 14
seguridad de bloqueo de la cubierta,
 precaución 26
bloqueo de la cubierta, inteligente 26
personalizar el software 2

D

integridad de datos 33
eliminar contraseña 21
caracteres delimitadores, tabla 21

herramientas de distribución, software 2
Desktop Management Interface (DMI) 13
herramienta de diagnóstico de unidades de
 disco duro 32
disco, clonar 2
DMI (Desktop Management Interface) 13
unidad, proteger 32
botón de alimentación dual 10

E

ahorro de energía, valores de 11
introducir
 contraseña de arranque 18
 contraseña de configuración 19

F

FailSafe Boot Block ROM 8
llave de seguridad
 precaución 28
 pedido 28
notificación de fallos 32
tecnología de identificación
 de huellas digitales 32
dar formato al disco,
 información importante 31

H

unidades de disco duro, herramienta de
 diagnóstico 32

I

configuración inicial 2
Intelligent Manageability 13
temperatura interna del equipo 33
direcciones de Internet, consulte sitios Web
ROM del sistema no válida 8

K

teclado nacional, caracteres
delimitadores 21
indicadores luminosos del teclado,
ROM, tabla 9

L

activar el bloqueo
de Smart Cover 27

M

seguridad del registro
de arranque maestro, valor 29

N

teclado nacional con
caracteres delimitadores 21

O

sistemas operativos, información
importante sobre 12
pedir llave de seguridad 28

P

crear particiones del disco,
información importante 31
contraseña
cambiar 20
borrar B-1
eliminar 21
de arranque B-1
de configuración 17, 19
contraseña de seguridad 17
PCN (Product Change
Notification) 6
botón de encendido
configurar 10
dual 10
Power Management 11
fuente de alimentación,
protector de sobretensión 33

contraseña de arranque

cambiar 20
eliminar 21
introducir 18
configurar 18

imagen de software preinstalada 2
Product Change Notification (PCN) 6
proteger la unidad de disco duro 32
proteger la ROM, precaución 7

R

sistema, recuperación 8
recuperación, software 2
memoria flash de la ROM remota 7
configuración remota 2
Remote System Installation, acceder 3
indicadores luminosos del teclado
de la ROM, tabla 9
ROM, no válida 8
ROM, actualizar 7

S

ahorrar energía 11
características de seguridad, tabla 15
valores de seguridad, configuración de 14
seguridad, registro de arranque maestro 29
valor
contraseña de arranque 18
contraseña de configuración 17, 19
sensor de Smart Cover 26
tiempos de espera 11
contraseña de configuración
cambiar 20
eliminar 21
introducir 19
configurar 17
configuración, inicial 2
configuración, replicar 10
Smart Cover, solicitar llave
de seguridad 28

bloqueo de Smart Cover
 bloquear 27
 desbloquear 27
 sensor de Smart Cover
 niveles de protección 25
 configurar 26
 software
 Altiris eXpress 3
 AssetControl 14
 utilidades de Computer Setup 10
 sistema de protección de unidades 32
 FailSafe Boot Block ROM 8
 notificación y recuperación
 de fallos 32
 integración 2
 seguridad del registro
 de arranque maestro 29
 Power Management 11
 recuperación 2
 memoria flash de la
 ROM remota 7
 Remote System Installation 2
 System Software Manager 6
 actualizar varias máquinas 6
 SSM (System Software Manager) 6
 fuente de alimentación
 con protector de sobretensión 33
 recuperación del sistema 8

System Software
 Manager (SSM) 6

T

interna, temperatura del equipo 33
 sensor térmico 33
 tiempos de espera, configuración 11

U

seguimiento de la integridad
 de discos Ultra ATA 33
 desactivar el bloqueo de Smart Cover 27
 actualizar la ROM 7
 URL (páginas Web).
 Consulte páginas Web

W

páginas Web
 www.compaq.com 7, 12, 28
 www.compaq.com/activeupdate 6
 www.compaq.com/easydeploy 4, 5, 7, 10, 12
 www.compaq.com/im/ssmwp.html 6, 7
 www.compaq.com/pcn 6
 www.compaq.com/products/quickspecs/10690_na/10690_na.html 32
 www.compaq.com/solutions/pcsolutions 2
 tecnologías Wired for Management 13
 direcciones de Internet.
 Consulte páginas Web